CLAIMS:

1. A method of enabling revocation or authorization of screened content material (100') screened by a screening device (103) or a screening application (103), the method comprising the step of:

- attaching or relating a unique screening device or application identifier (105) to content material (100) during import of the content material (100) from a non-compliant domain (101) into a compliant domain (102),

where the identifier (105) uniquely identifies the screening device (103) or the screening application (103) used to import said content material (100).

2. Method according to claim 1, characterized in that said method further comprises the step of generating and/or maintaining a revocation list (106) comprising a unique identifier (105) for at least one screening device or application (103) that has been determined to illegally import content material (100) into the compliant domain (102).

3. Method according to claim 2, characterized in that the method further comprises the step of

- checking in a use device or application (104) prior to use of a screened content material (100') whether said attached or related unique screening device or application identifier (105) exists in said revocation list (106), and disable the use of the screened content material (100') if this is the case.

4. Method according to claim 1, characterized in that the method further comprises the steps of:

- generating and/or maintaining an authorization list (106) comprising a unique identifier (105) for at least one screening device or application (103) that has been granted authorization to import content material (100) into the compliant domain (102), and

- checking in a use device or application (104) prior to use of a screened content material (100') whether said attached or related unique screening device or application

identifier (105) of a content material (100) exists in said authorization list (106), and disable use of the content material (100') if this is not the case.

5. Method according to claims 1 - 4, characterized in that the step of attaching or relating said unique identifier (105) comprises:

- obtaining screening information,
- obtaining additional information being dependent on at least part the content material (100), and
- digitally signing the screening information and additional information, resulting in a digital signature, that uniquely identifies the screening device (103) or application (103) used to import said content material (100).

6. Method according to claim 5, characterized in that said additional information comprises a result of a hash function performed on at least a part of said content material (100).

7. Method according to claim 5 or 6, characterized in that said additional information comprises a result of a digital fingerprint function performed on at least a part of said content material (100).

8. Method according to claims 5 – 7, characterized in that the method further comprises one or more steps of:

- checking said content material (100') for the existence of said screening and additional information , and
- checking for a correct digital signature over said screening information, where the steps of checking are performed prior to use of the content material (100') by a use device or application (104), and where said use is prevented if at least one check is not met.

9. Method according to claims 5 – 8, characterized in that said unique identifier (105) comprises at least a public key of a screening device (103) or screening application (103), which is signed by a trusted authority.

10. Method according to claims 5 – 9, characterized in that a unique identifier (105) of a recording device (104) is attached or related to a copy of the screened content

material (100') when the content material is recorded after import into the compliant domain (102).

11. Method according to claims 5 – 10, characterized in that said additional information includes:

- a representation of a time-stamp, and

that a use of said screened content (100') is disabled only if said time–stamp is

- after a time-stamp of the entry of said unique screening device or screening application identifier (105) in an authorization list (106), or
- after a time-stamp of the entry of said unique screening device or screening application identifier (105) in a revocation list (106).

12. A system for enabling revocation or authorization of screened content material (100') by a screening device (103) or a screening application (103), wherein

- the screening device or application (103) comprises means (302, 303, 304) for attaching or relating a unique screening device or application identifier (105) to the content material (100) during import of the content material (100) from a non-compliant domain (101) into a compliant domain (102),

where the identifier (105) uniquely identifies the screening device (103) or the screening application (103) used to import said content material (100).

13. A system according to claim 12, characterized in that said system further comprises means (107) for generating and/or maintaining a revocation list (106) comprising a unique identifier (105) for at least one screening device or application (103) that has been determined to illegally import content material (100) into the compliant domain (102).

14. A system according to claim 13, characterized in that the system further comprises a use device or application (104) adapted to

- check, prior to use of a screened content material (100'), whether said attached or related unique screening device or application identifier (105) exists in said revocation list (106), and disable the use of the screened content material (100') if this is the case.

15. A system according to claim 12, characterized in that the system further comprises:

- means (107) for generating and/or maintaining an authorization list (106) comprising a unique identifier (105) for at least one screening device or application (103) that has been granted authorization to import content material (100) into the compliant domain (102), and
- a use device or application (104) adapted to check, prior to use of a screened content material (100'), whether said attached or related unique screening device or application identifier (105) of a content material (100) exists in said authorization list (106), and disable the use of the content material (100') if this is not the case.

16. A system according to claims 12 - 15, characterized in that said means (302, 303, 304) for attaching or relating said unique identifier (105) comprises:
- means (302) for obtaining screening information,
- means (303) for obtaining additional information being dependent on at least a part the content material (100), and
means (304) for digitally signing the screening information and additional information, resulting in a digital signature, that uniquely identifies the screening device (103) or application (103) used to import said content material (100).

17. A system according to claim 16, characterized in that said additional information comprises a result of a hash function performed on at least a part of said content material (100) and/or a result of a digital fingerprint function performed on at least a part of said content material (100).

18. A system according to claims 16 – 17, characterized in that said use device or application (104) further is adapted, prior to use of a screened content material (100'), to:
- check said content material (100') for the existence of said screening and additional information, and
- check for a correct digital signature over said screening information
where said use is prevented if at least one check is not met.

19. A system according to claims 16 – 18, characterized in that said unique identifier (105) comprises at least a public key of a screening device (103) or screening application (103), which is signed by a trusted authority.

20. A system according to claims 16 – 19, characterized in that said system further comprises means (302, 303, 304) attaching or relating a unique identifier (105) of a recording device (104) to a copy of the screened content material (100') when the content material is recorded after import into the compliant domain (102).

21. A system according to claims 14 – 20, characterized in that said additional information includes:

- a representation of a time-stamp, and

that a use of said screened content (100') is disabled only if said time–stamp is

- after a time-stamp of the entry of said unique screening device or screening application identifier (105) in a authorization list (106), or
- after a time-stamp of the entry of said unique screening device or screening application identifier (105) in a revocation list (106).

22. A screening device (103) for enabling revocation or authorization of screened content material (100'), wherein

- the screening device comprises means (302, 303, 304) for attaching or relating a unique screening device or application identifier (105) to the content material (100) during import of the content material (100) from a non-compliant domain (101) into a compliant domain (102),

where the identifier (105) uniquely identifies the screening device (103) used to import said content material (100).

23. A use device (104) adapted to

- check, prior to a use of a screened content material (100'), what use right a unique screening device or application identifier (105) attached or related to said content material (100') signifies, and process said screened content material (100') according to said use right, where
- the content material (100') is imported by a screening device (103) adapted to attach or relate a unique screening device or application identifier (105) to the content material (100) during import of the content material (100) from a non-compliant domain (101) into a compliant domain (102).

24. A device according to claim 23, characterized in that said device is adapted to perform said check according to:

- checking whether said identifier (105) exists in a revocation list (106), and disable said use of the screened content material (100') if this is the case, where the revocation list (106) comprises a unique identifier (105) for at least one screening device or application (103) that has been determined to illegally import content material (100) into the compliant domain (102).

25. A device according to claim 23, characterized in that said device is adapted to perform said check according to:

- checking whether said identifier (105) exists in an authorization list (106), and disable use of the content material (100') if this is not the case, where the authorization list (106) comprises a unique identifier (105) for at least one screening device or application (103) that has been granted authorization to import content material (100) into the compliant domain (102).

26. A computer readable medium having stored thereon instructions for causing one or more processing units to execute the method according to any one of claims 1 – 11.